The Computer Support Newsletter

April 2005 http://msa.ars.usda.gov/computerhelp email news: sntucker@msa-stoneville.ars.usda.gov

Computer Support Newsletter Audience
A note to our many readers...... This newsletter is published mainly to inform MSA employees of Information Technology (IT) news and happenings. Much of the newsletter will relate to the local user base. If you are NOT at Stoneville, some of the contained items may not be relevant to you.

Evaluating Your Web Browser's Security Settings

Check the security settings in your web browser to make sure they are at an appropriate level. While increasing your security may affect the functionality of some web sites, it could prevent you from being attacked.

Why are security settings for web browsers important?
Your web browser is your primary connection to the rest of the internet, and multiple applications may rely on your browser, or elements within your browser, to function. This makes the security settings within your browser even more important. Many web applications try to enhance your browsing experience by enabling different types of functionality, but this functionality might be unnecessary and may leave you susceptible to being attacked. The safest policy is to disable the majority of those features unless you decide they are necessary. If you determine that a site is trustworthy, you can choose to enable the functionality temporarily and then disable it once you are finished visiting the site.

Where can you find the settings?
Each web browser is different, so you may have to look around. In Internet Explorer, you can find them by clicking **Tools** on your menu bar, selecting **Internet Options...**, choosing the **Security** tab, and clicking the **Custom Level...** button. Browsers have different security options and configurations, so familiarize yourself with the menu options, check the help feature, or refer to the vendor's web site.

While every application has settings that are selected by default, you may discover that your browser also has predefined security levels that you can select. For example, Internet Explorer offers custom settings that allow you to select a particular level of security; features are enabled or disabled based on your selection.

It is helpful to have an understanding of what the different terms mean so that you can evaluate the features to determine which settings are appropriate for you.

How do you know what your settings should be?
Ideally, you would set your security for the highest level possible. However, restricting certain features may limit some web pages from loading or functioning properly. The best approach is to adopt the highest level of security and only enable features when you require their functionality.

What do the different terms mean?
Different browsers use different terms, but here are some terms and options you may find:

- **Zones** - Your browser may give you the option of putting web sites into different segments, or zones, and allow you to define different security restrictions for each zone.

  For example, Internet Explorer identifies the following zones:

  Internet - This is the general zone for all public web sites. When you browse the internet, the settings for this zone are automatically applied to the sites you visit. To give you the best protection as you browse,

This newsletter is published by the ARS-USDA Mid-South Area Computer Support Staff. If you have news items, updates, corrections, or questions, please contact us via our email address or web site.

you should set the security to the highest level; at the very least, you should maintain a medium level.

Local intranet - If you are in an office setting that has its own intranet, this zone contains those internal pages. Because the web content is maintained on an internal web server, it is usually safe to have less restrictive settings for these pages. However, some viruses have tapped into this zone, so be aware of what sites are listed and what privileges they are being given.

Trusted sites - If you believe that certain sites are designed with security in mind, and you feel that content from the site can be trusted not to contain malicious materials, you can add them to your trusted sites and apply settings accordingly. Even if you trust them, avoid applying low security levels to external sites—if they are attacked, you might also become a victim.

Restricted sites - If there are particular sites you think might not be safe, you can identify them and define heightened security settings.

- **Pop-up Blocker** - Although turning this feature on could restrict the functionality of certain web sites, it will also minimize the number of pop-up ads you receive, some of which may be malicious. ***Remember if you are an ARIS or PCMS user, you can leave the pop-up blocker enabled, but you have to make an exception for USDA sites by entering *.usda.gov.***

Because the security settings may not be enough to protect you, the best precaution is to avoid navigating to any sites that make you question whether or not they're safe. You should also try using a browser other Internet Explorer. One of the more poplar browsers is Mozilla.

Understanding Cookies and Active Content

Many people browse the Internet without much thought to what is happening behind the scenes. Active content and cookies are common elements that may pose hidden risks when viewed in a browser or email client.

What are cookies?

When you browse the Internet, information about your computer may be collected and stored. This information might be general information about your computer (such as IP address, the domain you used to connect, and the type of browser you used). It might also be more specific information about your browsing habits (such as the last time you visited a particular web site or your personal preferences for viewing that site).

Cookies can be saved for varying lengths of time:

- Session cookies - Session cookies store information only as long as you're using the browser; once you close the browser, the information is erased. The primary purpose of session cookies is to help with navigation, such as by indicating whether or not you've already visited a particular page and retaining information about your preferences once you've visited a page.
- Persistent cookies - Persistent cookies are stored on your computer so that your personal preferences can be retained. In most browsers, you can adjust the length of time that persistent cookies are stored. It is because of these cookies that your email address appears by default when you open your Yahoo or Hotmail email account, or your personalized home page appears when you visit your favorite online merchant.

If an attacker gains access to your computer, he or she may be able to gather personal information about you through these files.

To increase your level of security, consider adjusting your privacy and security settings to block or limit cookies in your web browser. To make sure that other sites are not collecting personal information about you without your knowledge, choose to only allow cookies for the web site you are visiting; block or limit cookies from a third-party.

If you are using a public computer, you should make sure that cookies are disabled to prevent other people from accessing or using your personal information.

What is active content?

To increase functionality or add design embellishments, web sites often rely on scripts that execute programs within the web browser. This active content can be used to create "splash pages" or options like drop-down menus. Unfortunately, these scripts are often a way for attackers to download or execute malicious code on a user's computer.

- *JavaScript* - JavaScript is just one of many web scripts and is probably the most recognized. Used on almost every web site now, JavaScript and other scripts are popular because users expect the functionality and "look" that it provides, and it's easy to incorporate. However, because of these reasons, attackers can manipulate it to their own purposes. A popular type of attack that relies on JavaScript involves redirecting users from a legitimate web site to a malicious one that may download viruses or collect personal information.

- *Java and ActiveX controls* - Different from JavaScript, Java and ActiveX controls are actual programs that reside on your computer or can be downloaded over the network into your browser. If executed by attackers, untrustworthy ActiveX controls may be able to do anything on your computer that you can do (such as running spyware to collect personal information, connecting to other computers, and potentially doing other damage). Java applets usually run in a more restricted environment, but if that environment isn't secure, then malicious Java applets may create opportunities for attack as well.

- *Plug-ins* - Sometimes browsers require the installation of additional software known as plug-ins to provide additional functionality. Like Java and ActiveX controls, plug-ins may be used in an attack, so before installing them, make sure that they are necessary and that the site you have to download them from is trustworthy.

JavaScript and other forms of active content are not always dangerous, but they are common tools for attackers. You can prevent active content from running in most browsers, but realize that the added security may limit functionality and break features of some sites you visit. Before clicking on a link to a web site that you are not familiar with or do not trust, take the precaution of disabling active content.

Agency News

eTravel

The current method of booking Federal travel has changed. SATO has been selected to replace the Travel Management Centers (TMC) that were previously used to book travel for ARS. This is the first step in implementing eTravel throughout ARS. ARS is scheduled to have eTravel fully implement by October 2005.

SATO can be contacted directly on 877-698-2472. This number is available 24 hours per day. When contacting SATO, they will ask you to verify the correct E-mail address for the traveler. The correct E-mail address is necessary to ensure that the ticket information and itinerary are sent to the person traveling. Therefore, when making reservations for another, please ensure that you have their current and correct e-mail address and ensure that the information is validated with the SATO representative. If you and the SATO agent validate that the e-mail address is correct, no additional action is necessary.

If you determine that the E-mail address for the traveler is NOT correct, you must contact either Marcus Reinhold on 504-426-5672 or Ann Rumley Briggs on 504-426-5664 and ensure the traveler's profile is updated to reflect the correct e-mail address. **THE SATO AGENT CAN NOT MAKE THESE CHANGES TO THE TRAVELER'S PROFILE. THEY CAN ONLY VALIDATE INFORMATION.**

If SATO does not have a travel profile for the traveler, it's because that person has not sucessfully eAuthenticated. **ANYONE WHO HAS NOT EAUTHENTICATED, SHOULD DO SO AS SOON AS POSSIBLE.** You can find more on eAuthentication and instructions here.

Coming Soon - STARWeb
STARWEB is a real-time Web-based application for Time and Attendance Reporting. It will be used by unit timekeepers to prepare, print, and transmit time and attendance reports (T&As) to be sent to NFC for processing.

MSA plans to begin using STARWEB early this summer. Training for all timekeepers and backup timekeepers is in the planning stages. Dates and details will be released to all timekeepers when training plans are finalized.

MSA-HelpDesk
In our efforts to respond to your needs in a more efficient manner, Area Computer Support has implemented a new help policy.

Please email all IT needs or issues to MSA-HelpDesk@ars.usda.gov .

This email ID will forward to the MSA IT staff and will ensure that your issues are dealt with in as quickly a manner as possible.

Coming Soon to Stoneville - Complex Passwords

The Area Computer Office is in the process of testing a new Windows Domain Controller. In accordance with the USDA Security Policy, the new domain controller will require each user to use complex passwords at login. A few of the specific password requirements will be:

- Must be 8 characters
- Will require uppercase letters, lowercase letters and number mixtures
- Will remember last 20 passwords
- Will not allow sequencing (tucker01, tucker02,…)
- Can not change password more than once in 24 hours

You can find more information on password security in the April 2004 newsletter.

Tips and Tricks

Windows XP – Get Icons for CATS, PCMS and Discoverer

Groupwise 6.02 - User Manual

Microsoft Word – Turning off the Spell-Checker

Microsoft Excel – Printing column titles on every page

Microsoft Power Point- Making Presentation Files Smaller

Comments and Contacts:

Email your comments to:
sntucker@msa-stoneville.ars.usda.gov